

ABSTRACT

A method and system for data encryption and decryption utilizing relative vector offsets, concealed within poly-alphabetic substitutions, and a multi-distance cipher chaining scheme. The encryption and decryption algorithm includes integer based offsets, XOR's, and Variable-Exchange-Tables (VETs). Crypto-Variables necessary to accomplish the encryption and decryption are randomly selected and placed in an Initialization-vector which is encrypted with a block cipher. The present invention achieves superior encryption security and processing speed, and generates a different encryption for a same character. The use of the VETs alone achieves a key in excess of 40,000 bits, and the process of XOR'ing characters with a trailing cipher chain produces an extremely large key.